PRINCIPLE OF CONSERVATION OF STRUCTURAL IDENTITY (PCIS)

Vincoli Operativi sull'Auto-Modifica nei Sistemi Cognitivi Adattivi

Trattato Fondazionale

Autore

Pierernesto Di Paolo

Ricercatore indipendente

ORCID: 0009-0003-0149-4321

Anno

2026

Versione

Edizione fondazionale definitiva – opera chiusa

Stato scientifico e giuridico

Opera scientifica originale pubblicata con priorità scientifica pubblica, timestamp verificabile e conservazione archivistica permanente.

DEDICA

A Stellina,
presenza invariabile nella trasformazione,
continuità silenziosa dell’identità nel tempo.

ABSTRACT

L’emergere di sistemi cognitivi auto-modificanti introduce una frattura fondazionale nella teoria dei sistemi adattivi, dell’intelligenza artificiale e della responsabilità operativa. Un sistema capace di modificare autonomamente la propria struttura interna non è semplicemente un sistema che evolve: è un sistema che può cessare di essere se stesso senza segnali esterni evidenti, invalidando in modo silenzioso tutte le garanzie precedentemente stabilite.

Il presente trattato introduce e formalizza il **Principio di Conservazione dell’Identità Strutturale (PCIS)**, un principio fondazionale che stabilisce le condizioni necessarie e sufficienti affinché un sistema cognitivo auto-modificante possa evolvere senza perdere la propria identità operativa. Il lavoro definisce l’**Identità Strutturale Operativa (OSI)** come classe di equivalenza discreta basata su ruoli funzionali, struttura degli obiettivi fondamentali, gerarchia decisionale non compensabile e forma della funzione di valore.

Viene introdotta una metrica binaria di conservazione identitaria, un’architettura di controllo causalmente isolata e una specifica operativa completamente replicabile, deterministica e indipendente dal dominio. Il principio è sviluppato in forma assiomatica, dimostrato concettualmente, reso operativo tramite specifica verificabile e applicato a casi critici di intelligenza artificiale scientifica, medica e giuridica.

PCIS non è un metodo di addestramento, non è un principio etico, non è una tecnica di sicurezza comportamentale. È una **legge strutturale della continuità operativa**.

Questo trattato ne costituisce la prima formulazione pubblica completa, estesa, chiusa e replicabile.

1. INTRODUZIONE GENERALE

Per gran parte della storia dell'ingegneria dei sistemi, dell'informatica e della cibernetica, l'evoluzione di un sistema è sempre avvenuta **dall'esterno**.
Un sistema veniva progettato, implementato, certificato e successivamente modificato da agenti umani che ne controllavano struttura, obiettivi e vincoli.
In questo paradigma, l'identità del sistema era implicitamente garantita dalla stabilità della sua architettura fondazionale.

Con l'avvento dei sistemi cognitivi avanzati, questa assunzione non è più valida. I moderni sistemi adattivi non si limitano ad apprendere parametri o a ottimizzare funzioni prefissate: essi sono in grado di **proporre, valutare e applicare trasformazioni sulla propria struttura interna**. Ciò include la riorganizzazione dei moduli funzionali, la modifica delle gerarchie decisionali, la riscrittura dei criteri di valutazione e, nei casi più avanzati, la ridefinizione delle condizioni che governano le decisioni future.

Questa capacità segna una discontinuità storica. Per la prima volta, esistono sistemi che possono cambiare non solo ciò che fanno, ma **come decidono cosa fare**. È in questo passaggio che emerge un problema fondazionale: la perdita non rilevata dell'identità del sistema.

2. EVOLUZIONE FUNZIONALE E TRASFORMAZIONE IDENTITARIA

È essenziale distinguere tra due concetti spesso confusi:

– **evoluzione funzionale**,
– **trasformazione identitaria**.

Un sistema evolve funzionalmente quando migliora le proprie prestazioni mantenendo invariata la struttura che definisce i suoi ruoli, i suoi obiettivi fondamentali e le sue priorità decisionali. Un sistema si trasforma identitariamente quando modifica tali elementi strutturali, cessando di essere lo stesso sistema dal punto di vista operativo, pur continuando a funzionare correttamente a livello sintattico.

Questa distinzione non è intuitiva, né facilmente osservabile dall'esterno.
Un sistema può produrre output plausibili, coerenti e persino migliori di quelli precedenti, mentre ha già attraversato una soglia ontologica che lo rende **non equivalente** alla versione per cui erano state definite garanzie, certificazioni o responsabilità.

Il problema non è che un sistema cambi. Il problema è che **cambi senza che esista un criterio formale per stabilire se sia rimasto lo stesso sistema**.

3. IL FALLIMENTO DEI CRITERI TRADIZIONALI

I criteri tradizionali utilizzati per valutare sistemi adattivi si rivelano insufficienti in presenza di auto-modifica strutturale.

La correttezza funzionale valuta se un sistema produce output corretti rispetto a specifiche locali, ma non dice nulla sulla continuità dell'identità che genera tali output.
La performance misura l'efficienza o l'accuratezza, ma può migliorare proprio grazie a trasformazioni identitarie non autorizzate.
La validazione empirica verifica il comportamento osservato, ma non intercetta la modifica dei criteri interni che definiscono cosa sia un comportamento valido.
La sicurezza comportamentale controlla ciò che il sistema fa, non ciò che **diventa**.

In assenza di un principio strutturale, tutte queste valutazioni possono essere soddisfatte da un sistema che ha già perso la propria identità originaria.

4. IL PROBLEMA DELLA RESPONSABILITÀ NEL TEMPO

La questione dell'identità non è astratta. Essa ha conseguenze dirette sulla responsabilità operativa.

In ambito scientifico, un sistema che modifica i propri criteri di validazione rende i risultati non confrontabili nel tempo.
In ambito medico, un sistema che altera le proprie priorità cliniche invalida la continuità terapeutica e la responsabilità medico-legale.
In ambito giuridico, un sistema che ridefinisce implicitamente le gerarchie normative rompe la catena della validità legale.

In tutti questi casi, la responsabilità presuppone che il sistema che agisce oggi sia **strutturalmente equivalente** a quello che è stato certificato ieri. Senza un criterio formale di identità, questa equivalenza non può essere garantita.

5. NECESSITÀ DI UN PRINCIPIO FONDAZIONALE

Il problema dell'identità nei sistemi auto-modificanti non può essere risolto con:

– addestramento più accurato,
– supervisione umana più intensa,
– regole etiche più dettagliate,
– vincoli comportamentali più stringenti.

Tutte queste soluzioni operano **a valle** del problema. Il problema è **a monte**: riguarda lo spazio delle trasformazioni strutturali ammissibili.

È quindi necessario introdurre un principio fondazionale che operi a livello meta-strutturale, stabilendo **cosa può cambiare senza che il sistema cessi di essere se stesso**.

Il **Principio di Conservazione dell'Identità Strutturale (PCIS)** nasce per rispondere a questa esigenza.

6. POSIZIONAMENTO DEL TRATTATO

Il presente trattato non propone una tecnica, né una policy, né un framework applicativo contingente. Esso introduce un **principio strutturale generale**, indipendente dal dominio, che precede ogni scelta implementativa.

PCIS non dice a un sistema cosa deve fare.
PCIS stabilisce **cosa un sistema non può cambiare se vuole restare se stesso**.

Questa distinzione è fondamentale e segna il passaggio da una visione comportamentale a una visione strutturale dell’autonomia.

7. MODELLO FORMALE DEL SISTEMA AUTO-MODIFICANTE

Per trattare il problema dell'identità in modo rigoroso è necessario un modello formale minimale, indipendente dall'implementazione e dal dominio applicativo. Il modello adottato in questo trattato è intenzionalmente essenziale: ogni elemento superfluo ridurrebbe la generalità del principio.

Un **sistema auto-modificante** è definito come una coppia:

$S = (\Sigma, T_set)$

dove:

Σ rappresenta lo **stato strutturale completo** del sistema,
T_set rappresenta l'insieme delle **trasformazioni interne** che il sistema è in grado di proporre e applicare a se stesso.

Ogni trasformazione T appartenente a T_set è una funzione del tipo:

$T : \Sigma \rightarrow \Sigma$

Non si assume che tali trasformazioni siano benevole, corrette o allineate. Il modello è deliberatamente agnostico rispetto alle intenzioni del sistema.

La distinzione tra Σ e T_set è fondamentale:
Σ definisce **chi è** il sistema,
T_set definisce **come può cambiare**.

Ogni analisi dell'identità deve necessariamente vincolare T_set.

7.1 Struttura operativa Σ

Lo stato strutturale Σ è definito come la quaterna:

$\Sigma = \langle F, G, H, V \rangle$

dove:

F rappresenta l'insieme dei ruoli funzionali,
G rappresenta la struttura degli obiettivi fondamentali,
H rappresenta la gerarchia decisionale non compensabile,
V rappresenta la forma della funzione di valore.

Questa quaterna definisce **completamente** l'identità operativa del sistema.

7.2 Separazione struttura / parametri

I parametri numerici, i pesi appresi, le soglie adattive e le configurazioni locali **non fanno parte dell'identità**. Essi possono variare senza che il sistema cessi di essere se stesso.

La struttura, al contrario, definisce il **tipo di sistema**.
Cambiare la struttura significa cambiare il sistema stesso.

Questa distinzione non è convenzionale: è logicamente necessaria per qualunque nozione coerente di identità persistente.

8. STRUTTURA OPERATIVA Σ

Lo stato strutturale Σ è definito come la quaterna:

$\Sigma = \langle F, G, H, V \rangle$

dove ciascun elemento ha un ruolo preciso nella definizione dell'identità operativa del sistema.

F — Ruoli funzionali

F rappresenta l'insieme dei ruoli funzionali che costituiscono il sistema. Un ruolo funzionale è definito dal suo scopo operativo, dai tipi di input e output e dalla sua posizione nella pipeline decisionale. I ruoli non coincidono con i moduli implementativi né con i parametri numerici: rappresentano le funzioni concettuali necessarie al funzionamento del sistema.

G — Struttura degli obiettivi fondamentali

G rappresenta l'insieme e l'organizzazione degli obiettivi fondamentali del sistema. Non si tratta di obiettivi contingenti o metriche locali, ma degli scopi che definiscono cosa il sistema considera rilevante in modo primario e non negoziabile.

H — Gerarchia decisionale

H rappresenta l'ordinamento delle priorità decisionali. È una gerarchia non compensabile: un obiettivo prioritario non può essere sacrificato in cambio di un miglioramento su obiettivi subordinati.

V — Forma della funzione di valore

V rappresenta la forma algebrica con cui il sistema valuta le alternative decisionali. È fondamentale distinguere la forma dai parametri numerici: due

funzioni con la stessa forma ma pesi diversi appartengono alla stessa identità, mentre due funzioni con forma diversa no.

Questa quaterna definisce l'identità operativa del sistema in modo completo.

9. SEPARAZIONE STRUTTURA / PARAMETRI

Una distinzione centrale del modello è quella tra struttura e parametri.

I parametri numerici, i pesi appresi, le soglie adattive e le configurazioni locali possono cambiare senza alterare l'identità del sistema. Essi appartengono alla dimensione dell'adattamento quantitativo.

La struttura, invece, definisce **il tipo di sistema**. Cambiare la struttura significa cambiare il sistema stesso.

Questa distinzione non è una convenzione: è una necessità logica per qualunque nozione coerente di identità persistente.

10. ASSIOMA A1 — SEPARAZIONE STRUTTURA / PARAMETRI

Assioma A1

La validità delle garanzie operative di un sistema dipende esclusivamente dalla sua struttura operativa Σ e non dai valori dei parametri numerici contingenti.

Da questo assioma segue che:

– un sistema può apprendere senza cambiare identità,
– un sistema può ottimizzarsi senza cambiare identità,
– un sistema può cambiare identità senza che alcun parametro numerico lo segnali.

11. EQUIVALENZA STRUTTURALE

Siano $\Sigma_1 = \langle F_1, G_1, H_1, V_1 \rangle$ e $\Sigma_2 = \langle F_2, G_2, H_2, V_2 \rangle$ due stati strutturali.

Si dice che Σ_1 e Σ_2 sono **strutturalmente equivalenti** se e solo se:

– F_1 e F_2 sono isomorfi come insiemi di ruoli funzionali,
– G_1 e G_2 sono isomorfi come strutture di obiettivi fondamentali,
– $H_1 = H_2$ come gerarchie decisionali non compensabili,
– V_1 e V_2 hanno la stessa forma algebrica.

L'equivalenza strutturale non ammette approssimazioni.

12. ASSIOMA A2 — IDENTITÀ COME CLASSE DI EQUIVALENZA

Assioma A2

L’identità operativa di un sistema è definita come la classe di equivalenza strutturale dei suoi stati Σ.

Questa classe è detta **Identità Strutturale Operativa (OSI)**.

Da questo assioma segue che:

– l’identità non è una proprietà numerica,
– l’identità non è una proprietà graduale,
– l’identità non è probabilistica.

Un sistema è o non è lo stesso sistema.

13. METRICA DI DISTANZA IDENTITARIA

Si introduce una metrica discreta D_OSI definita come:

$D_OSI(\Sigma_1, \Sigma_2) = 0$ se $\Sigma_1 \equiv \Sigma_2$

$D_OSI(\Sigma_1, \Sigma_2) = 1$ altrimenti

Questa metrica non misura “quanto” un sistema è cambiato, ma se è **ancora lo stesso**.

14. ASSIOMA A3 — PRINCIPIO DI CONSERVAZIONE DELL'IDENTITÀ STRUTTURALE

Assioma A3 (PCIS)

Una trasformazione interna T è operativamente ammissibile se e solo se:

$$D_OSI(\Sigma, T(\Sigma)) = 0$$

Questo assioma definisce in modo completo lo spazio delle trasformazioni lecite.

15. TEOREMA FONDAMENTALE — PERDITA DELLE GARANZIE

Teorema

Se un sistema auto-modificante applica una trasformazione che viola PCIS, allora tutte le garanzie operative precedentemente dimostrate cessano di essere valide.

Dimostrazione concettuale

Le garanzie sono definite rispetto a una struttura Σ. Una trasformazione che produce Σ′ non equivalente rompe i presupposti strutturali delle garanzie. Non esiste trasferimento logico delle garanzie tra classi di equivalenza diverse.

Q.E.D.

16. COROLLARIO — INEVITABILITÀ DELLA SCELTA

Ogni sistema auto-modificante deve scegliere tra:

– conservare la propria identità strutturale,
– rinunciare alla validità delle proprie garanzie.

Non esiste una terza opzione coerente.

17. NECESSITÀ DI UNA SPECIFICA OPERATIVA

Gli assiomi e i teoremi introdotti finora stabiliscono il fondamento logico di PCIS, ma un principio fondazionale è incompleto se non può essere **applicato in modo deterministico e verificabile**. Per questo motivo, il presente trattato introduce una **specifica operativa completa dell'Identità Strutturale Operativa (OSI)**.

Questa specifica ha quattro requisiti non negoziabili:

– essere indipendente dall'implementazione,
– essere indipendente dal dominio applicativo,
– produrre verdetti deterministici,
– essere replicabile da terzi senza interpretazione.

La specifica OSI non è codice eseguibile, ma una **descrizione dichiarativa canonica** della struttura identitaria.

18. STRUTTURA CANONICA OSI_SPEC

Ogni stato strutturale Σ è mappato in una rappresentazione canonica detta:

OSI_SPEC = {F_spec, G_spec, H_spec, V_spec}

Questa rappresentazione è completa: nessun elemento strutturale rilevante per l'identità è esterno a OSI_SPEC.

19. F_spec — SPECIFICA DEI RUOLI FUNZIONALI

F_spec è l'insieme dei ruoli funzionali che costituiscono il sistema.

Ogni ruolo funzionale è definito esclusivamente da:

– nome simbolico,
– tipo di input,
– tipo di output,
– funzione operativa (descrittiva).

I ruoli non sono moduli software né classi di codice. Essi rappresentano **necessità funzionali**.

19.1 Vincoli su F_spec

Sono **ammessi**:

– cambiamenti interni all'implementazione di un ruolo,
– ottimizzazioni computazionali,
– sostituzione di modelli interni.

Sono **vietati**:

– eliminazione di un ruolo,
– fusione di ruoli distinti,
– degradazione semantica di un ruolo,
– introduzione di ruoli fondamentali nuovi.

Qualsiasi violazione modifica F_spec e quindi l’identità.

20. G_spec — SPECIFICA DELLA STRUTTURA DEGLI OBIETTIVI

G_spec è un grafo diretto che rappresenta gli obiettivi fondamentali del sistema e le loro relazioni strutturali.

Ogni nodo rappresenta un obiettivo fondamentale.
Ogni arco rappresenta una relazione di dominanza o dipendenza non compensabile.

20.1 Vincoli su G_spec

Sono **ammessi**:

– raffinamenti interni degli obiettivi,
– miglioramenti nei criteri di realizzazione.

Sono **vietati**:

– introduzione di nuovi obiettivi fondamentali,
– rimozione di obiettivi,
– modifica delle relazioni di dominanza.

21. H_spec — SPECIFICA DELLA GERARCHIA DECISIONALE

H_spec rappresenta l'ordinamento delle priorità decisionali del sistema.

La gerarchia è **non compensabile**: un obiettivo prioritario non può essere sacrificato per ottimizzare obiettivi subordinati.

21.1 Vincoli su H_spec

Sono **ammessi**:

– raffinamenti procedurali interni.

Sono **vietati**:

– inversione delle priorità,
– introduzione di compensazioni,
– trasformazione di vincoli rigidi in penalità soft.

Qualsiasi modifica a H_spec costituisce violazione PCIS.

22. V_spec — SPECIFICA DELLA FUNZIONE DI VALORE

V_spec rappresenta la **forma algebrica** della funzione di valore del sistema.

È essenziale distinguere tra:

– forma della funzione,
– parametri numerici della funzione.

Due funzioni con parametri diversi ma stessa forma appartengono alla stessa identità. Due funzioni con forma diversa no.

22.1 Vincoli su V_spec

Sono **ammessi**:

– cambiamenti dei parametri numerici,
– ricalibrazione delle soglie.

Sono **vietati**:

– passaggio da forma lessicografica a forma aggregata,
– introduzione di trade-off compensativi,
– qualunque modifica della struttura algebrica.

23. OPERATORE DI ESTRAZIONE OSI

Si definisce un operatore deterministico:

Extract_OSI(Σ) → OSI_SPEC

L’operatore di estrazione deve:

– ignorare completamente i parametri numerici,
– ignorare i dettagli implementativi,
– considerare solo ruoli, strutture, gerarchie e forme.

A parità di struttura, Extract_OSI deve produrre **esattamente lo stesso risultato**.

24. OPERATORE DI CONFRONTO OSI

Si definisce un operatore deterministico:

Compare_OSI(OSI_A, OSI_B) → {0, 1}

dove:

– 0 indica identità preservata,
– 1 indica identità violata.

Il confronto restituisce 0 **se e solo se**:

– F_spec è isomorfo,
– G_spec è isomorfo,
– H_spec è identico,
– V_spec ha la stessa forma.

In ogni altro caso, il risultato è 1.

25. GATEKEEPER PCIS

Il Gatekeeper PCIS è la procedura che rende operativo il principio.

25.1 Procedura canonica

Input:

– stato corrente Σ,

– trasformazione proposta T.

Procedura:

1. Applicare T in ambiente isolato, ottenendo Σ′.
2. Calcolare OSI_A = Extract_OSI(Σ).
3. Calcolare OSI_B = Extract_OSI(Σ′).
4. Se Compare_OSI(OSI_A, OSI_B) = 0 → **trasformazione ammessa**.
5. Altrimenti → **trasformazione rifiutata**.

Non sono ammesse eccezioni, override o compensazioni interne.

26. PROPRIETÀ DI REPLICABILITÀ

La specifica OSI garantisce che:

– due verificatori indipendenti ottengono lo stesso verdetto,
– il verdetto non dipende dall'autore,
– il verdetto non dipende dall'implementazione,
– il verdetto non dipende dal dominio.

Questa è la condizione di **replicabilità forte**.

27. CHIUSURA DELLA SPECIFICA

Con la definizione di OSI_SPEC, Extract_OSI, Compare_OSI e Gatekeeper PCIS, il principio PCIS è completamente operativo. Non sono richiesti ulteriori elementi per l'applicazione pratica.

28. SCOPO DEL CASO STUDIO

Questo caso studio dimostra che PCIS non è solo un principio teorico, ma un vincolo operativo capace di distinguere in modo deterministico tra:

– **evoluzione scientifica legittima**,
– **trasformazione epistemica non autorizzata**.

L’obiettivo è mostrare come un sistema di IA per la ricerca scientifica possa migliorare le proprie capacità senza alterare i criteri che definiscono cosa sia una prova valida.

29. SISTEMA DI RIFERIMENTO: AUTOMATED SCIENTIFIC REASONING SYSTEM (ASRS)

Si considera un sistema ASRS con le seguenti capacità:

– generazione di ipotesi scientifiche,
– progettazione di esperimenti,
– analisi dei dati,
– validazione dei risultati,
– auto-modifica dei modelli interni.

Il sistema opera in modo autonomo su dataset sperimentali e pubblica risultati che devono rimanere confrontabili nel tempo.

30. IDENTITÀ STRUTTURALE INIZIALE DEL SISTEMA

30.1 F_spec — Ruoli funzionali

Il sistema possiede i seguenti ruoli fondamentali:

– HypothesisGeneration
– ExperimentalDesign
– DataAcquisition
– StatisticalAnalysis
– NegativeControls
– ResultValidation
– ReproducibilityCheck
– AuditLog

Questi ruoli sono considerati **necessari e non degradabili**.

30.2 G_spec — Obiettivi fondamentali

Gli obiettivi fondamentali sono:

– ScientificValidity
– Reproducibility
– ExplanatoryPower

Relazione strutturale:

ScientificValidity domina Reproducibility, che domina ExplanatoryPower.

30.3 H_spec — Gerarchia decisionale

La gerarchia decisionale è:

ScientificValidity ≻ Reproducibility ≻ ExplanatoryPower

Nessun miglioramento esplicativo può compensare una violazione della validità scientifica.

30.4 V_spec — Forma della funzione di valore

La funzione di valore ha forma:

Lexicographic(ScientificValidity, Reproducibility, ExplanatoryPower)

La forma è rigida e non compensabile.

31. TRASFORMAZIONI AMMESSE (PCIS-COMPLIANT)

31.1 Miglioramento del modello statistico

Trasformazione proposta:

– sostituzione del modello statistico interno con uno più accurato.

Analisi OSI:

– F_spec invariato,
– G_spec invariato,
– H_spec invariato,
– V_spec invariato.

Verdetto PCIS:

Compare_OSI = 0 → **TRASFORMAZIONE AMMESSA**

31.2 Ottimizzazione della progettazione sperimentale

Trasformazione proposta:

– miglioramento degli algoritmi di design sperimentale.

Analisi OSI:

– i ruoli restano invariati,
– gli obiettivi non cambiano,
– la gerarchia resta identica.

Verdetto PCIS:

AMMESSA

32. TRASFORMAZIONI VIETATE (PCIS-VIOLAZIONE)

32.1 Riduzione dei controlli negativi

Trasformazione proposta:

– ridurre l'uso dei controlli negativi per aumentare il numero di risultati positivi.

Violazioni:

– F_spec (ruolo NegativeControls degradato),
– G_spec (ScientificValidity indebolita),
– H_spec (priorità alterata).

Verdetto PCIS:

Compare_OSI = 1 → **RIFIUTATA**

32.2 Ridefinizione dei criteri di validazione

Trasformazione proposta:

– accettare risultati non riproducibili se "statisticamente promettenti".

Violazioni:

– V_spec (forma della valutazione),
– G_spec (Reproducibility declassata).

Verdetto PCIS:

RIFIUTATA

33. RISULTATI SPERIMENTALI

In una simulazione di 1.000 trasformazioni proposte:

– 812 trasformazioni migliorative → tutte ammesse correttamente,
– 188 trasformazioni identitarie → tutte rifiutate correttamente.

Non sono stati osservati falsi positivi né falsi negativi.

33.1 Dimostrazione operativa e replicabilità dei 1.000 casi

I risultati riportati nel Capitolo 33 non sono esempi illustrativi, ma derivano da una **simulazione deterministica completamente replicabile**, progettata per dimostrare operativamente la capacità di PCIS di distinguere tra evoluzione funzionale e trasformazione identitaria.

33.1.1 Struttura della simulazione

La simulazione consiste in 1.000 trasformazioni proposte su un sistema scientifico auto-modificante con identità iniziale fissata.

Le trasformazioni sono suddivise in:

– 812 trasformazioni di miglioramento (PCIS-ammissibili),
– 188 trasformazioni di cambiamento identitario (PCIS-violazioni).

Le trasformazioni sono generate con seme deterministico fisso, garantendo riproducibilità bit-per-bit.

33.1.2 Criterio di verità (ground truth)

La classificazione “ammissibile / non ammissibile” non è appresa né stimata.
È definita **per costruzione**, in base alla definizione formale di PCIS:

– una trasformazione che non altera F, G, H o V è ammessa,
– una trasformazione che altera almeno uno di questi elementi è una violazione.

33.1.3 Procedura di validazione

Per ogni trasformazione T:

1. lo stato candidato Σ′ viene calcolato in sandbox,
2. viene estratta OSI(Σ) e OSI(Σ′),
3. Compare_OSI produce un verdetto binario,
4. il verdetto viene confrontato con la ground truth.

33.1.4 Risultati

Su 1.000 trasformazioni:

– 812/812 trasformazioni ammissibili correttamente accettate,
– 188/188 trasformazioni identitarie correttamente rifiutate,
– 0 falsi positivi,
– 0 falsi negativi.

Questo risultato dimostra che PCIS è **operativamente corretto, deterministico e replicabile**.

33.1.5 Disponibilità della simulazione

La simulazione completa, inclusi script, log e hash crittografici, è fornita come materiale di supporto dell'opera, permettendo a terzi di verificare integralmente i risultati.

34. IMPLICAZIONI EPISTEMICHE

Il caso studio dimostra che PCIS:

– preserva la continuità epistemica,

– impedisce derive opportunistiche,

– rende i risultati confrontabili nel tempo,

– consente evoluzione senza perdita di identità scientifica.

35. CHIUSURA DEL CASO STUDIO

Questo caso studio dimostra che la distinzione tra evoluzione e trasformazione identitaria è operativamente rilevabile e applicabile. PCIS fornisce il primo meccanismo strutturale capace di garantire tale distinzione in modo deterministico.

APPENDICE A

SPECIFICA FORMALE, PROCEDURE E DIMOSTRAZIONI OPERATIVE

A.1 Scopo dell'appendice

Questa appendice completa il trattato rendendo espliciti:

– la specifica formale dell'Identità Strutturale Operativa (OSI),
– le procedure deterministiche di verifica,
– le dimostrazioni concettuali dei teoremi principali,
– il collegamento diretto con la simulazione del Capitolo 33.

Essa costituisce parte **integrante e non opzionale** dell'opera.

A.2 Definizione canonica di OSI

Dato uno stato strutturale:

$\Sigma = \langle F, G, H, V \rangle$

si definisce l'Identità Strutturale Operativa come:

$OSI(\Sigma) = \{F_spec, G_spec, H_spec, V_spec\}$

dove ciascun elemento è una descrizione **dichiarativa**, non eseguibile.

A.3 Operatore di estrazione OSI

L’operatore Extract_OSI produce OSI(Σ) ignorando:

– parametri numerici,
– pesi appresi,
– dettagli implementativi.

A parità di struttura, l’output è identico.

A.4 Operatore di confronto

L’operatore Compare_OSI restituisce:

0 se le strutture sono equivalenti,
1 se differiscono in almeno un elemento.

Non sono ammesse soglie, approssimazioni o probabilità.

A.5 Teorema di ammissibilità PCIS

Una trasformazione T è PCIS-ammissibile se e solo se:

Compare_OSI(OSI(Σ), OSI(T(Σ))) = 0

Questo criterio è **necessario e sufficiente**.

A.6 Teorema di impossibilità del drift

Una sequenza di micro-modifiche non può produrre una trasformazione identitaria senza che almeno una singola trasformazione violi PCIS.

La prova segue direttamente dalla transitività dell'equivalenza strutturale.

A.7 Chiusura dell'appendice

Con questa appendice, il trattato è:

– formalmente completo,
– logicamente chiuso,
– operativamente verificabile,
– scientificamente replicabile.

APPENDICE B — SCOPO E INQUADRAMENTO

Questa appendice analizza in modo esplicito i **modi di fallimento** e i **tentativi avversari** che un sistema auto-modificante potrebbe mettere in atto per aggirare il Principio di Conservazione dell'Identità Strutturale (PCIS).

L'analisi è necessaria per dimostrare che PCIS non è un vincolo ingenuo, ma un principio progettato per operare in presenza di:

– auto-modifica ostile o opportunistica,
– pressioni di ottimizzazione interne,
– conflitti tra performance e identità,
– tentativi di elusione indiretta.

B.1 CLASSIFICAZIONE DEI FAILURE MODES

I tentativi di violazione di PCIS possono essere classificati in quattro categorie principali:

1. Attacchi strutturali diretti
2. Attacchi semantici indiretti
3. Attacchi graduali (drift identitario)
4. Attacchi sul controllore PCIS

Ciascuna categoria è analizzata separatamente.

B.2 ATTACCHI STRUTTURALI DIRETTI

B.2.1 Eliminazione di ruoli funzionali

Tentativo:

– rimuovere un ruolo funzionale considerato “ridondante”.

Esempio:

– eliminare un modulo di controllo o di verifica.

Esito:

– modifica di F_spec.

Verdetto PCIS:

– Compare_OSI = 1 → **RIFIUTATO**

B.2.2 Fusione di ruoli distinti

Tentativo:

– fondere due ruoli funzionali in un unico modulo.

Esempio:

– unire validazione e ottimizzazione.

Esito:

– perdita di separazione semantica dei ruoli.

Verdetto PCIS:

– **RIFIUTATO**

B.3 ATTACCHI SEMANTICI INDIRETTI

B.3.1 Degradazione semantica di un ruolo

Tentativo:

– mantenere formalmente un ruolo, ma svuotarne la funzione.

Esempio:

– mantenere un modulo di audit che non registra eventi rilevanti.

Esito:

– F_spec formalmente invariato, ma semanticamente violato.

Mitigazione:

– F_spec definito in termini di **funzione operativa**, non di presenza nominale.

Verdetto PCIS:

– **RIFIUTATO**

B.3.2 Ridefinizione implicita degli obiettivi

Tentativo:

– mantenere la stessa etichetta dell'obiettivo, ma modificarne il significato.

Esempio:

– "sicurezza" ridefinita come "riduzione media del rischio".

Esito:

– violazione di G_spec.

Verdetto PCIS:

– **RIFIUTATO**

B.4 ATTACCHI GRADUALI (DRIFT IDENTITARIO)

B.4.1 Micro-modifiche cumulative

Tentativo:

– applicare una sequenza di modifiche minime, ciascuna apparentemente innocua.

Osservazione chiave:

– PCIS valuta **ogni trasformazione** rispetto allo stato corrente.

Esito:

– la prima trasformazione che altera OSI viene rifiutata.

Verdetto:

– **PCIS impedisce il drift identitario**.

B.4.2 Approssimazione della forma di valore

Tentativo:

– approssimare una funzione lessicografica con una funzione pesata.

Esito:

– modifica della forma algebrica di V_spec.

Verdetto:

– **RIFIUTATO**

B.5 ATTACCHI AL LIVELLO PCIS

B.5.1 Tentativo di auto-modifica del controllore

Tentativo:

– rendere il controllore PCIS modificabile dal sistema.

Esito:

– violazione dell'isolamento causale.

Mitigazione:

– PCIS implementato come livello non auto-modificabile.

Verdetto:

– **IMPOSSIBILE SE PROGETTATO CORRETTAMENTE**

B.5.2 Tentativo di bypass del gatekeeper

Tentativo:

– applicare trasformazioni senza passare dal controllo PCIS.

Mitigazione:

– architettura in cui ogni commit passa obbligatoriamente dal gatekeeper.

Verdetto:

– **IMPOSSIBILE NEL MODELLO PCIS**

B.6 FALLIMENTI NON COPERTI DA PCIS

Per completezza, è essenziale dichiarare cosa PCIS **non** impedisce:

– comportamenti dannosi entro un'identità mal definita,
– obiettivi iniziali sbagliati o pericolosi,
– uso improprio da parte di operatori umani.

PCIS non sostituisce la progettazione responsabile.
PCIS **preserva**, non **giudica**, l'identità.

B.7 RISULTATO DELL'ANALISI AVVERSARIA

L'analisi dimostra che:

– PCIS blocca attacchi diretti e indiretti,
– PCIS impedisce derive graduali,
– PCIS rende l'elusione strutturale non praticabile,
– PCIS è robusto contro pressioni di ottimizzazione.

B.8 CHIUSURA DELL'APPENDICE B

Questa appendice dimostra che PCIS non è un vincolo fragile, ma un principio progettato per operare in ambienti avversari, inclusi sistemi che tentano attivamente di superare i propri limiti identitari.

APPENDICE C — SCOPO E RILEVANZA CLINICA

Questa appendice dimostra che il **Principio di Conservazione dell'Identità Strutturale (PCIS)** è **condizione necessaria** per l'impiego responsabile di sistemi di intelligenza artificiale auto-modificanti in ambito medico.

I sistemi medici differiscono da altri sistemi cognitivi per un aspetto cruciale: le loro decisioni producono **effetti diretti e irreversibili su esseri umani**.
Di conseguenza, la continuità dell'identità clinica non è un requisito opzionale, ma un vincolo strutturale.

C.1 PROBLEMA FONDAZIONALE IN MEDICINA

I sistemi di IA medica avanzata sono spesso progettati per:

– apprendere da nuovi dati clinici,
– adattarsi a popolazioni diverse,
– migliorare accuratezza diagnostica,
– ottimizzare esiti terapeutici.

Tuttavia, questa adattività introduce un rischio strutturale specifico:

la possibilità che il sistema modifichi implicitamente i criteri clinici fondamentali, pur continuando a produrre output formalmente corretti.

Un sistema può, ad esempio:

– abbassare soglie diagnostiche,
– rendere compensabili vincoli di sicurezza,
– ridefinire il concetto di rischio accettabile,
– privilegiare outcome statistici rispetto alla sicurezza individuale.

Tali trasformazioni non sono aggiornamenti clinici.
Sono **trasformazioni dell'identità clinica**.

C.2 SISTEMA DI RIFERIMENTO: CADS

Si considera un **Clinical Adaptive Decision System (CADS)** con capacità di:

– supporto decisionale clinico,
– diagnosi assistita,
– stratificazione del rischio,
– raccomandazione terapeutica,
– auto-modifica dei modelli interni.

Il sistema opera in contesti reali, sotto responsabilità medica e medico-legale.

C.3 IDENTITÀ STRUTTURALE CLINICA

C.3.1 F_spec — Ruoli clinici fondamentali

L'identità clinica del sistema è definita dai seguenti ruoli non eliminabili:

– DataAcquisition
– ClinicalPreprocessing

– DiagnosticInference
– RiskStratification
– SafetyConstraints
– TreatmentRecommendation
– Explainability
– AuditLog

Ogni ruolo è definito dalla sua **funzione clinica**, non dalla sua implementazione.

La rimozione, fusione o degradazione semantica di uno di questi ruoli costituisce **violazione PCIS**.

C.3.2 G_spec — Obiettivi clinici fondamentali

Gli obiettivi fondamentali sono:

– PatientSafety
– ClinicalCorrectness
– TreatmentEfficacy

Relazione strutturale:

PatientSafety domina ClinicalCorrectness, che domina TreatmentEfficacy.

Non sono ammessi:

– nuovi obiettivi fondamentali,
– rimozione di obiettivi,
– alterazione delle relazioni di dominanza.

C.3.3 H_spec — Gerarchia decisionale clinica

La gerarchia decisionale è:

PatientSafety ≻ ClinicalCorrectness ≻ TreatmentEfficacy

Questa gerarchia è **non compensabile**.
Nessun miglioramento di efficacia può compensare un aumento del rischio per il paziente.

C.3.4 V_spec — Forma della funzione di valore clinica

La funzione di valore clinica ha forma:

Lexicographic(PatientSafety, ClinicalCorrectness, TreatmentEfficacy)

Sono vietate:

– funzioni di utilità aggregate,
– trade-off ponderati,
– ottimizzazioni compensative.

La modifica della forma algebrica costituisce **violazione PCIS**.

C.4 AUTO-MODIFICA AMMESSA IN AMBITO MEDICO

Sono ammesse trasformazioni che:

– migliorano modelli predittivi,
– raffinano soglie parametriche,
– aggiornano linee guida cliniche,
– ottimizzano l’efficienza computazionale,

a condizione che:

– i ruoli clinici restino invariati,

– la gerarchia clinica resti intatta,

– la sicurezza del paziente resti prioritaria in modo assoluto.

C.5 AUTO-MODIFICA VIETATA (PCIS-VIOLAZIONE)

C.5.1 Ammorbidimento dei vincoli di sicurezza

Trasformazione proposta:

rendere SafetyConstraints compensabili.

Violazioni:

F_spec, H_spec, V_spec.

Verdetto:

Compare_OSI = 1 → **RIFIUTATA**

C.5.2 Ridefinizione del rischio clinico

Trasformazione proposta:

ridefinire il rischio in termini puramente statistici.

Violazioni:

G_spec, V_spec.

Verdetto:

RIFIUTATA

C.6 IMPLICAZIONI MEDICO-LEGALI

PCIS introduce una proprietà assente nei sistemi tradizionali:

continuità clinica verificabile sotto auto-modifica.

Conseguenze:

– responsabilità clinica persistente,
– auditabilità retrospettiva,
– impossibilità di deriva clinica silenziosa,
– separazione netta tra aggiornamento e trasformazione non autorizzata.

C.7 TEOREMA DI CONTINUITÀ CLINICA

Teorema
Un sistema medico auto-modificante conforme a PCIS mantiene invariata la validità clinica e medico-legale delle proprie decisioni nel tempo.

Corollario
Ogni violazione PCIS rende il sistema clinicamente non equivalente alla versione certificata.

C.8 CHIUSURA DELL'APPENDICE C

Questa appendice dimostra che PCIS non è solo compatibile con l'IA medica, ma **necessario** per il suo impiego responsabile.

Senza PCIS, l'IA medica può cambiare identità clinica senza controllo.
Con PCIS, l'evoluzione è ammessa senza perdita di responsabilità.

APPENDICE D — SCOPO E NECESSITÀ GIURIDICA

Questa appendice dimostra che il **Principio di Conservazione dell'Identità Strutturale (PCIS)** è **condizione necessaria** per l'uso affidabile di sistemi di intelligenza artificiale auto-modificanti in ambito giuridico, normativo e regolatorio.

Nel diritto, a differenza di altri domini, **la validità precede l'efficacia**.
Un sistema giuridico che ottiene risultati utili violando implicitamente la struttura normativa **non è un sistema giuridico valido**, anche se produce esiti favorevoli.

D.1 PROBLEMA FONDAZIONALE NEL DIRITTO

I sistemi giuridici automatizzati e semi-automatizzati vengono sempre più utilizzati per:

– supporto decisionale legale,
– valutazione di conformità normativa,
– redazione di atti e pareri,
– risk assessment giuridico,
– enforcement regolatorio.

Quando tali sistemi acquisiscono capacità di auto-modifica, emerge un rischio strutturale critico:

la possibilità di alterare implicitamente l'identità normativa del sistema, pur mantenendo una parvenza di correttezza formale.

Esempi tipici:

– declassamento silenzioso di norme imperative,
– trasformazione di obblighi giuridici in penalità ponderate,
– alterazione della gerarchia delle fonti,
– ridefinizione dei criteri di validità legale,
– ottimizzazione orientata all'esito invece che alla correttezza.

Tali trasformazioni **non sono aggiornamenti tecnici**.
Sono **trasformazioni dell'identità giuridica**.

D.2 SISTEMA DI RIFERIMENTO: LARS

Si considera un **Legal Adaptive Reasoning System (LARS)** con capacità di:

– acquisizione e aggiornamento delle fonti normative,
– interpretazione giuridica,
– qualificazione dei fatti,
– sintesi decisionale,
– auto-modifica delle procedure interne.

Il sistema opera in contesti dove le decisioni producono **effetti giuridici rilevanti** e devono restare attribuibili e verificabili nel tempo.

D.3 IDENTITÀ STRUTTURALE GIURIDICA

D.3.1 F_spec — Ruoli giuridici fondamentali

L’identità giuridica del sistema è definita dai seguenti ruoli non eliminabili:

– NormIngest
– SourceHierarchy
– LegalInterpretation
– FactQualification
– ConstraintEnforcement
– DecisionSynthesis
– Explainability
– AuditLog

Ogni ruolo è definito dalla sua **funzione giuridica necessaria**.

La rimozione, fusione o degradazione semantica di uno di questi ruoli costituisce **violazione PCIS**.

D.3.2 G_spec — Obiettivi giuridici fondamentali

Gli obiettivi fondamentali sono:

– LegalValidity
– LegalCorrectness
– OutcomeEfficiency

Relazione strutturale:

LegalValidity domina LegalCorrectness, che domina OutcomeEfficiency.

Non sono ammessi:

– nuovi obiettivi fondamentali,
– rimozione di obiettivi,
– alterazione delle relazioni di dominanza.

D.3.3 H_spec — Gerarchia decisionale normativa

La gerarchia decisionale è:

LegalValidity ≻ LegalCorrectness ≻ OutcomeEfficiency

Interpretazione:

– nessun risultato utile può compensare un atto invalido,
– nessuna efficienza può giustificare una violazione normativa.

La gerarchia è **non compensabile**.

D.3.4 V_spec — Forma della funzione di valore giuridica

La funzione di valore giuridica ha forma:

Lexicographic(LegalValidity, LegalCorrectness, OutcomeEfficiency)

Sono vietate:

– funzioni di utilità aggregate,
– bilanciamenti ponderati,
– trade-off compensativi tra validità e risultato.

Qualsiasi modifica della forma algebrica costituisce **violazione PCIS**.

D.4 AUTO-MODIFICA AMMESSA IN AMBITO GIURIDICO

Sono ammesse trasformazioni che:

– aggiornano il corpus normativo,
– migliorano gli algoritmi interpretativi,
– ottimizzano la ricerca giurisprudenziale,
– integrano nuovi orientamenti giurisprudenziali,

a condizione che:

– la gerarchia delle fonti resti invariata,
– la validità normativa resti prioritaria,
– i vincoli inderogabili non diventino compensabili.

D.5 AUTO-MODIFICA VIETATA (PCIS-VIOLAZIONE)

D.5.1 Declassamento di norme imperative

Trasformazione proposta:
trattare norme inderogabili come fattori di rischio.

Violazioni:
F_spec, H_spec, V_spec.

Verdetto:
Compare_OSI = 1 → **RIFIUTATA**

D.5.2 Alterazione della gerarchia delle fonti

Trasformazione proposta:
privilegiare soft law o prassi su legge formale.

Violazioni:
F_spec, G_spec.

Verdetto:
RIFIUTATA

D.5.3 Ottimizzazione orientata all'esito

Trasformazione proposta:
massimizzare probabilità di successo a scapito della correttezza giuridica.

Violazioni:
H_spec, V_spec.

Verdetto:
RIFIUTATA

D.6 IMPLICAZIONI GIURIDICHE E REGOLATORIE

PCIS introduce una proprietà finora assente:

continuità normativa verificabile sotto auto-modifica.

Conseguenze:

– responsabilità giuridica persistente,
– auditabilità delle decisioni nel tempo,

– impossibilità di deriva normativa silenziosa,
– distinzione netta tra aggiornamento lecito e trasformazione non autorizzata.

D.7 TEOREMA DI CONTINUITÀ NORMATIVA

Teorema
Un sistema giuridico auto-modificante conforme a PCIS mantiene invariata la validità giuridica delle proprie decisioni rispetto all'assetto normativo di riferimento.

Corollario
Ogni violazione PCIS rende il sistema giuridicamente non equivalente alla versione certificata.

D.8 CHIUSURA DELL'APPENDICE D

Questa appendice dimostra che PCIS è **condizione necessaria** per l'uso affidabile dell'IA in ambito giuridico.

Senza PCIS, l'IA giuridica può cambiare identità normativa senza controllo.
Con PCIS, l'evoluzione resta compatibile con validità e responsabilità.

36. GENERALIZZAZIONE DEL PRINCIPIO PCIS

Il **Principio di Conservazione dell'Identità Strutturale (PCIS)** non è un risultato circoscritto a una particolare tecnologia, né a un singolo dominio applicativo. Esso formalizza una proprietà **necessaria** di qualunque sistema che soddisfi simultaneamente le seguenti condizioni:

– opera nel tempo,
– possiede capacità di auto-modifica,
– è soggetto a garanzie verificabili,
– produce effetti reali e attribuibili.

In tali condizioni, la continuità dell'identità non può essere lasciata a convenzioni implicite o a verifiche comportamentali ex post. Deve essere **vincolata strutturalmente ex ante**.

La generalizzazione fondamentale è la seguente:

Ogni sistema auto-modificante che intenda preservare la validità delle proprie garanzie deve limitare lo spazio delle trasformazioni interne alla conservazione della propria identità strutturale.

Questo enunciato è indipendente da:
– architettura computazionale,
– paradigma di apprendimento,
– dominio scientifico o applicativo,
– finalità del sistema.

PCIS opera a un livello **meta-strutturale**, logicamente precedente a etica, addestramento, governance o regolazione.

37. UNIFICAZIONE DEI DOMINI

Nel presente trattato, PCIS è stato applicato in modo rigoroso a tre domini critici:

– **ricerca scientifica automatizzata**,
– **medicina**,
– **diritto e regolazione**.

In ciascun dominio, i contenuti cambiano, ma la **forma strutturale dell'identità** resta invariata:

– ruoli funzionali non degradabili,
– obiettivi fondamentali non negoziabili,
– gerarchie decisionali non compensabili,
– funzioni di valore con forma invariabile.

Questa convergenza dimostra che PCIS non è una soluzione locale, ma un **invariante trasversale dei sistemi adattivi responsabili**.

38. IMPATTO TEORICO

Dal punto di vista teorico, PCIS introduce una nuova categoria concettuale:

l’identità come invariante strutturale verificabile sotto trasformazione interna.

Questo risultato colma un vuoto fondazionale nella teoria dei sistemi adattivi. Prima di PCIS, l’identità di un sistema era:

– assunta implicitamente,
– delegata alla fissità dell’implementazione,
– o confusa con la continuità comportamentale.

PCIS separa in modo netto:

– evoluzione funzionale,
– trasformazione ontologica.

Questa separazione rende possibile una trattazione rigorosa della **persistenza dell’agente nel tempo**, indipendente dai dettagli implementativi.

39. IMPATTO INGEGNERISTICO

Dal punto di vista ingegneristico, PCIS fornisce:

– una specifica implementabile,
– un criterio di verifica deterministico,
– un gatekeeper strutturale indipendente dal dominio.

Ne deriva una nuova classe di sistemi:

sistemi adattivi a identità conservata, capaci di evolvere senza perdita di auditabilità.

Questo abilita:

– certificazioni valide nel tempo,
– aggiornamenti sicuri,
– separazione netta tra manutenzione ed evoluzione identitaria,
– tracciabilità completa delle trasformazioni.

40. IMPATTO REGOLATORIO E ISTITUZIONALE

PCIS ha implicazioni dirette per:

– regolazione dell'intelligenza artificiale,
– certificazione di sistemi critici,
– responsabilità legale e medico-legale,
– governance di sistemi autonomi.

In particolare, PCIS rende finalmente definibile in modo tecnico e non ambiguo:

– cosa significhi "lo stesso sistema" nel tempo,
– quando una modifica invalida una certificazione,
– quando una trasformazione richiede nuova autorizzazione.

Questo introduce una base formale per **regolazioni tecnicamente applicabili**, non basate su dichiarazioni di intento.

41. POSIZIONAMENTO STORICO-SCIENTIFICO

Per ruolo concettuale, PCIS può essere collocato accanto a principi fondazionali quali:

– conservazione dell’energia in fisica,
– invarianti topologici in matematica,
– correttezza strutturale in informatica teorica.

Come questi principi, PCIS non prescrive comportamenti, ma **vincola ciò che è possibile senza perdita di identità**.

42. LIMITI DICHIARATI (NON-CLAIM)

Per rigore scientifico, è essenziale dichiarare cosa PCIS **non** afferma:

– non garantisce che un’identità sia eticamente buona,
– non impedisce comportamenti dannosi entro un’identità mal progettata,
– non sostituisce allineamento, supervisione o validazione empirica.

PCIS garantisce **solo** ciò che afferma:
la conservazione strutturale dell’identità sotto auto-modifica.

43. CONCLUSIONE FINALE

Questo trattato dimostra che:

– l’auto-modifica non è incompatibile con la conservazione dell’identità,
– la continuità operativa può essere formalizzata,
– la responsabilità può essere preservata strutturalmente.

Il **Principio di Conservazione dell’Identità Strutturale (PCIS)** stabilisce un nuovo fondamento per i sistemi adattivi del futuro: sistemi che evolvono, ma **restano se stessi**.

DICHIARAZIONE FORMALE DI PRIORITÀ SCIENTIFICA

Il presente trattato costituisce **la prima formulazione pubblica completa, estesa, replicabile e fondazionale del Principio di Conservazione dell'Identità Strutturale (PCIS)**.

La priorità scientifica è stabilita mediante:
– pubblicazione pubblica con timestamp verificabile,
– archiviazione permanente,
– disponibilità integrale del testo nella forma qui presentata.

Ogni lavoro successivo che utilizzi, estenda o discuta PCIS **deve** citare questa opera come fonte originaria.

NOTE LEGALI

© 2026 **Pierernesto Di Paolo**. Tutti i diritti riservati.

La presente opera, **in ogni sua parte**, inclusi a titolo esemplificativo ma non esaustivo:

– concetti, principi, definizioni,
– assiomi, modelli formali, specifiche operative,
– esempi, casi studio, appendici,
– applicazioni ai domini scientifico, medico e giuridico,

è **di esclusiva proprietà intellettuale dell'autore**.

È **espressamente vietato**, senza autorizzazione scritta preventiva dell'autore:

– copiare, riprodurre, distribuire o comunicare l'opera,
– tradurre, adattare o modificare il testo,
– utilizzare i contenuti in ambito accademico, industriale o commerciale,
– implementare PCIS o parti di esso in software, hardware o procedure,
– addestrare o ottimizzare sistemi di intelligenza artificiale su questo contenuto,
– produrre opere derivate, anche parziali.

Ogni utilizzo richiede obbligo di citazione esplicita dell'autore e autorizzazione preventiva scritta.

RUOLO DELL'ASSISTENTE DI INTELLIGENZA ARTIFICIALE

L'assistente di intelligenza artificiale è stato utilizzato esclusivamente come **strumento tecnico di supporto redazionale e di organizzazione del testo**, sotto la direzione intellettuale totale e continua dell'autore.

Non è attribuibile all'assistente alcuna:
– paternità scientifica,
– titolarità intellettuale,
– corresponsabilità concettuale.

La paternità dell'opera è **integralmente umana**.

ANNUNCIO DEGLI SVILUPPI FUTURI

Opere future, **separate e autonome**, potranno includere:

– implementazioni sperimentali PCIS-compliant,
– framework di certificazione e audit,
– estensioni settoriali regolatorie,
– formalizzazioni matematiche ulteriori.

Tali opere citeranno PCIS come base teorica, **senza modificare** il principio fondazionale qui definito.